SLOVENSKÁ AKREDITAČNÁ AGENTÚRA
PRE VYSOKÉ ŠKOLSTVO

VNÚTORNÝ PREDPIS Č. 8/2024

SMERNICA O RIADENÍ BEZPEČNOSTNÝCH INCIDENTOV SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO

V Bratislave 12. decembra 2024

SMERNICA O RIADENÍ BEZPEČNOSTNÝCH INCIDENTOV SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO

Výkonná rada Slovenskej akreditačnej agentúry pre vysoké školstvo (ďalej len „výkonná rada“) schválila dňa 12. decembra 2024 podľa čl. 9 ods. 1 písm. i) Štatútu Slovenskej akreditačnej agentúry pre vysoké školstvo (ďalej len „agentúra“) túto *Smernicu o riadení bezpečnostných incidentov Slovenskej akreditačnej agentúry pre vysoké školstvo* (ďalej len „smernica“).

Článok 1
Úvodné ustanovenia

1. Cieľom riadenia bezpečnostných incidentov v súvislosti s aktívami agentúry je ich včasná identifikácia, kategorizácia a optimálny postup pri ich riešení s ohľadom na minimalizáciu dopadov a škôd.

Článok 2
Vymedzenie pojmov

1. **Bezpečnostným incidentom** (ďalej aj „BI“) sa označuje okolnosť, udalosť alebo činnosť, ktorá má alebo by mohla mať v prípade svojho dokonania negatívny dopad na bezpečnosť aktív agentúry. Každý BI musí byť evidovaný a vyšetrený. BI môže byť spôsobený objektívnymi príčinami, konaním fyzických osôb alebo živelnou pohromou.
2. **Kategorizácia BI** podľa úrovní dopadov pre agentúru je uvedená v článku 6 tejto smernice.
3. **Podozrenie z BI** je taká okolnosť, udalosť alebo činnosť, ktorá vedie zamestnanca k záveru, že by mohlo byť ohrozené niektoré z aktív agentúry. Musí byť nahlásené, posúdené a vyšetrené v súlade s touto smernicou.
4. **Slabé miesto** je také miesto v informačnom systéme, v majetku, službe alebo činnosti, ktoré by mohlo byť zneužité na ohrozenie bezpečnosti aktív agentúry.
5. **Informačný systém** (ďalej aj „IS“) je súbor, sústava alebo databáza obsahujúca dáta alebo osobné údaje, ktoré sú systematicky spracúvané na dosiahnutie účelu spracúvania, a to za použitia automatizovaných alebo iných prostriedkov spracúvania.

Článok 3
Hlavné kategórie bezpečnostných incidentov

1. Medzi hlavné kategórie BI patria:
   a) v oblasti majetku agentúry najmä
   - krádež,
   - poškodenie alebo zničenie majetku,
   - neoprávnený pobyt v sídle agentúry,
   - násilné vniknutie do priestorov agentúry s následkom odcudzenia aktív agentúry;

   b) v oblasti informačnej a kybernetickej bezpečnosti najmä
   - zverejnenie alebo prezradenie hesla prístupových práv používateľa,
   - prístup neoprávnenej osoby do IS agentúry,
   - infiltrácia škodlivého softvéru (malvér, ransomvér a pod.) do IS agentúry,
   - pripojenie neschváleného hardvéru a inštalácia neschváleného softvéru do súčastí a komponentov IS agentúry,
   - nevykonávanie predpísaného zálohovania,
   - zničenie alebo odcudzenie médií, na ktorých sú dáta, resp. bezpečnostné zálohy,

- svojvoľné prepisovanie a úprava záznamov,
- spracúvanie osobných údajov v rozpore s príslušnou smernicou agentúry;

c) v oblasti zdravia zamestnancov najmä
- pracovný úraz,
- poškodenie elektrických zariadení, plynových a iných rozvodov alebo havárie, ktoré ohrozujú zdravie zamestnancov,
- konanie tretích osôb v priestoroch agentúry ohrozujúce zdravie zamestnancov.

Článok 4
Indikácia a postup pri podozrení na bezpečnostný incident

1. Zdroje indikácie BI v prípade, že je agentúra cieľom útoku, sú najmä:
   a) automatické hlásenie (napr. hlásenie zo systému na detekciu neoprávneného vniknutia a pod.),
   b) manuálna identifikácia (napr. ako výsledok bezpečnostnej analýzy, bezpečnostného auditu, resp. testov),
   c) oznámenie od zamestnanca agentúry,
   d) oznámenie od tretej osoby.
2. Každý zamestnanec agentúry, ktorý má podozrenie, že odhalil BI, odhalil slabé miesto alebo má podozrenie, že vývoj udalostí môže smerovať k BI, je povinný to bezodkladne oznámiť ústne, telefonicky alebo e-mailom vedúcemu kancelárie.
3. Pokiaľ ide o dôvodné podozrenie z BI, musí byť o ňom informovaný aj manažér kybernetickej bezpečnosti.
4. Na základe zistených informácií vedúci kancelárie v súčinnosti s manažérom kybernetickej bezpečnosti rozhodne, či ohlásené podozrenie z BI je skutočne bezpečnostným incidentom alebo ním nie je, a bude tak považované iba za podnet na zlepšenie úrovne všeobecnej bezpečnosti.

Článok 5
Riešenie bezpečnostného incidentu a jeho vyhodnotenie

1. Postup zamestnancov pri riešení BI musí smerovať najmä k (v tomto poradí dôležitosti):
   a) ochrane ľudského života a zdravia,
   b) ochrane aktív a minimalizácie strát agentúry,
   c) zaisteniu dôkazného materiálu a zisteniu skutočných príčin BI.
2. Pri riešení BI sa postupuje bezodkladne podľa úrovne jeho významnosti realizáciou činností a v časovom harmonograme podľa článku 6 tejto smernice.
3. Každý zamestnanec je pri riešení BI, jeho vyšetrení a odstraňovaní následkov povinný poskytnúť všetku súčinnosť.
4. Vedúci kancelárie je povinný zabezpečiť vyriešenie pracovnoprávnych dôsledkov BI (článok 6 ods. 2 tejto smernice), ak sú tieto odôvodnené.
5. Manažér kybernetickej bezpečnosti je v prípade potreby povinný zabezpečiť došetrenie BI pomocou forenznej analýzy.
6. Vedúci kancelárie v súčinnosti s manažérom kybernetickej bezpečnosti je po uzatvorení BI povinný informovať o výsledku predsedu výkonnej rady a primerane aj všetkých priamo či nepriamo angažovaných zamestnancov.
7. Vedúci kancelárie je povinný prijať, resp. iniciovať prijatie preventívnych administratívnych, technických, resp. personálnych opatrení na zabránenie opakovania BI.
8. O bezpečnostnom incidente sa vyhotoví záznam podľa príslušného tlačiva (príloha).

Článok 6
Matica hrozieb bezpečnostného incidentu a nadväzné aktivity

1. Matica hrozieb kategorizujúca úroveň významnosti BI podľa jeho dopadu na agentúru. Pri posudzovaní úrovne BI postačuje splnenie aj jedného dopadu:

Úroveň BI	**1**	**2**	**3**	**4**	**5**
Potenciálna hrozba BI	**Žiadny dopad**	**Kontrolovateľný dopad**	**Vážny dopad**	**Kritický dopad**	**Katastrofálny dopad**
Možný finančný dopad *	žiadna finančná strata	malá finančná strata (do 150 €)	stredná finančná strata (od 150 € do 1 500 €)	významná finančná strata (od 1 500 € do 15 000 €)	podstatná finančná strata (od 15 000 € do 150 000 €)
Možný dopad na vierohodnosť agentúry	žiadny	malé ohrozenie dôveryhodnosti	vážne ohrozenie dôveryhodnosti	vážna strata dôveryhodnosti	podstatná strata dôveryhodnosti
Úroveň obmedzenia služieb pre verejnosť	bez obmedzenia	minimálne obmedzenie poskytovania základnej služby	viditeľné obmedzenie poskytovania základnej služby	kritické obmedzenie poskytovania základnej služby	dlhodobý výpadok poskytovania základnej služby
Strata dôvery voči tretím stranám	žiadna	boli prezradené interné informácie	boli prezradené interné informácie a osobné údaje	boli prezradené citlivé informácie o XXYY a osobné údaje	boli prezradené strategické materiály, strata databáz osobných údajov

* Pod *finančným dopadom* sa rozumejú priame a nepriame náklady spojené s odstraňovaním následkov BI.

2. Činnosti, resp. aktivity, ktoré je potrebné vykonať pri BI podľa jeho úrovne:

Úroveň BI	**1**	**2**	**3**	**4**	**5**
Aktivity smerom k médiám a verejnosti	bez komentára	bez komentára	vyjadrenie pre verejnosť alebo médiá v prípade potreby	pripravené vyhlásenie pre médiá	pripravené vyhlásenie pre médiá
Úroveň manažmentu, ktorý je potrebné informovať	vedúci oddelenia	vedúci oddelenia	vedúci kancelárie	vedúci kancelárie + predseda výkonnej rady	vedúci kancelárie + predseda výkonnej rady
Možný personálny dopad v prípade dokázaného osobného zavinenia	dohovor, zhodnotenie pri osobnom hodnotiacom pohovore	dohovor, možné písomné upozornenie na porušenie prac.disciplíny, zhodnotenie pri osobnom pohovore	písomné porušenie pracovnej disciplíny	písomné porušenie pracovnej disciplíny	písomné porušenie pracovnej disciplíny

3. Časový harmonogram reakcie na BI v závislosti od úrovne BI, ak je možné ho v čase oznámenia zistiť, resp. odhadnúť:

Úroveň BI	1	2	3	4	5
Reakcia	do 5 prac. dní	do 3 prac. dní	do 1 prac. dňa	ihneď, riešenie BI je prioritou	ihneď, riešenie BI je prioritou

Článok 7
Nahlasovanie bezpečnostného incidentu
do Jednotného informačného systému kybernetickej bezpečnosti

1. Agentúra má povinnosť nahlasovať závažné kybernetické BI do Jednotného informačného systému kybernetickej bezpečnosti (ďalej len „JISKB“), ktorý je prevádzkovaný Národným bezpečnostným úradom (ďalej len „NBÚ“).
2. Kritériá na určenie závažného kybernetického BI sú definované vo Vyhláške č. 165/2018 Z. z. NBÚ, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických BI a podrobnosti hlásenia kybernetických BI.
3. Za nahlásenie BI do JISKB zodpovedá vedúci kancelárie a manažér kybernetickej bezpečnosti.

Článok 8
Záverečné ustanovenia

1. Táto smernica je záväzná pre všetkých zamestnancov agentúry, musia s ňou byť preukázateľne oboznámení a sú povinní ju dodržiavať.
2. Za dodržiavanie tejto smernice je zodpovedný vedúci kancelárie agentúry.
3. Výnimku z tejto smernice môže udeliť len predseda výkonnej rady agentúry, resp. ním poverený zástupca.
4. Pokiaľ sa niektoré ustanovenia tejto smernice stanú neplatnými alebo neúčinnými, nie je tým dotknutá platnosť a účinnosť celej smernice.
5. Na situácie neupravené touto smernicou sa primerane použijú ustanovenia súvisiacich všeobecne záväzných predpisov a vnútorných predpisov agentúry.
6. Výklad ustanovení tejto smernice je oprávnený poskytovať vedúci kancelárie.
7. Táto smernica nadobúda účinnosť schválením výkonnou radou agentúry dňa 12. 12. 2024.

V Bratislave 12. 12. 2024

prof. Ing. Robert Redhammer, PhD.
predseda výkonnej rady

Príloha: Záznam o bezpečnostnom incidente (BI)

Po vyplnení **dôverná** informácia

Formulár pre záznam o bezpečnostnom incidente (BI)	
Typ BI:	

Opis BI:	
Kategória BI:	

(podľa čl. 6)

BI oznámil: *(meno, lokalita)*	
Dňa:	

Mená zamestnancov podieľajúcich sa na riešení BI:	
Vykonané opatrenia: *(opis a dátum)*	
Navrhované opatrenia: *(vrátane termínov* *a zodpovedných zamestnancov)*	

Vyšetrenie BI ukončené dňa ..... Podpis .....